

**Office of the Chief Information Officer
Enterprise Policy**

Policy Number: CIO-078

Effective Date: 06/10/2003

Revision Date: 11/01/2005

Subject: Intranet Wireless Local Area Network (WLAN) Policy

Policy: The Commonwealth Office of Technology (COT) is responsible for ensuring the confidentiality, integrity, and availability of the Commonwealth's computing environment. The purpose of this policy is to outline security and data integrity measures required for secure wireless LAN installations within the state's intranet zone.

Policy Maintenance: The Office of the CIO has issued this Enterprise Policy. The Commonwealth Office of Technology (COT), Office of Infrastructure Services, is responsible for the maintenance of this policy. All agencies and employees within the Executive Branch of state government shall adhere to this policy. However, agencies may choose to add to this policy, in order to enforce more restrictive policies as appropriate. Therefore, employees are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy.

Responsibility for Compliance: Each agency is responsible for assuring that appropriate employees within its organizational authority have been made aware of the provisions of this policy, that compliance is expected, and that unauthorized and/or neglectful installations of wireless LANs that expose the Commonwealth's network infrastructure to intruders and/or attacks may result in disciplinary action pursuant to KRS 18A up to, and including dismissal.

Maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems. Therefore, it is important that agencies assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

An agency should not undertake wireless deployment for any operations until it has examined and can acceptably manage and mitigate the risks to its information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies because their unique security requirements will determine which products should be considered for purchase.

It is the responsibility of each Cabinet and agency to enforce and manage this policy. Failure to comply may result in additional shared service charges to the agency for COT's efforts to remediate issues related to insecure wireless LAN installations. Failure to comply may also result in termination of access to the network infrastructure.

Procedures:

Before implementation, all customers that utilize the Kentucky Information Highway (KIH) must have installation approval by COT, Office of Infrastructure Services for any intranet wireless LAN. At this time, the Commonwealth Office of Technology recommends the use of wireless network technology only as a solution for special or unique business requirements and not for general-purpose deployment.

Enterprise Standards:

The following security standards and network configurations are required for all intranet wireless LAN installations:

- The placement of wireless LAN Access Points (WAP) must be strategically located to prevent the interception of wireless signals by unauthorized individuals or outside the intended coverage area. WAPs should be mounted above ceiling tiles, out of plain site, or otherwise publicly inaccessible and not visible to

unauthorized persons. The range of WAPs must also be tested to ensure that signals are not being transmitted outside the intended coverage area.

- All WAP installations must use the strongest native standard of encryption available (128 bit is recommended) for the device, usually Wired Equivalent Privacy (WEP).
- All WAP configuration parameters (Service Set Identifier (SSID), keys, passwords, channels, etc) that can be changed from the default manufacturer settings must be changed from the default. Also, the beacon interval on the WAP must be set to the longest interval possible. Where applicable, the new settings should be complex and not easily discerned or provide clues to the location, agency, or data / system description. Passwords must conform to password composition rules as stated in the [Commonwealth's Enterprise UserID and Password Policy](#), CIO-072.
- WAP connections must be restricted to only identified, expected, listed, and known Message Authentication Code (MAC) addresses.
- WAP keys must be changed on a periodic basis.
- WAPs must not be connected to a LAN's hub instead of a switch. An Ethernet hub will transmit data to every node on the network, including the wireless LAN segment. An intruder will not only be able to see data transmitted over the wireless LAN but also from the LAN.
- WAP connections must be restricted to only identified, expected, listed, and known Message Authentication Code (MAC) addresses.
- Physical security of wireless WAPs must be maintained to protect the WAP from theft or access to the data port.
- The wireless LAN must utilize SSID (Service Set Identifier). SSID distinguishes one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. The SSID should not openly identify the LAN or its purpose, and should be constructed as securely as a password.
- WEP (Wired Equivalent Privacy) must be enabled on all WAPs and devices in order to prevent the SSID from being transmitted as clear text.
- It is crucial that WEP be used in conjunction with SSID and MAC address filtering.
- Due to multiple security flaws in WEP, a wireless LAN must be supplemented with a virtual private network (VPN) solution. VPN clients should be installed on all attached devices.
- Firewalls must be installed between wireless and traditional LANs and must implement a block all, allow few rule set.
- Sensitive/confidential data must not be transmitted via wireless LANs unless strong cryptography ([128 bit TripleDES](#)) is used. Agencies should consider the content of email messages that may contain such confidential information.
- All security measures implemented for traditional, non-public LANs, including adequate encryption and authentication mechanisms, must also be utilized for wireless LAN installations.

The following wireless security best practices should be reviewed and considered by agencies before deployment and during operation of a wireless LAN:

- All WAP installations should be inventoried and the area in which the wireless LAN is installed must be regularly inspected for unauthorized WAPs or other devices not part of the approved installation. The network should be regularly inspected both physically and electronically using sniffing tools to uncover rogue WAPs and devices.
- Dynamic Host Configuration Protocol (DHCP) on wireless networks is strongly discouraged. DHCP can provide automatic IP network identification to any wireless device.
- If available, disable regular broadcasting of the SSID or other identifying broadcast information from the WAP.
- WAP configuration settings should be periodically assessed to ensure security mechanisms are being properly implemented. There are various tools on the market that can be used for capturing WAP configurations.

- Periodic security reviews should be conducted to ensure that changes to the wireless LAN have not exposed the network to intruders. In addition, the network should be periodically scanned to detect unauthorized devices.
- Strong, two-factor authentication or better should be considered for user authentication.
- Software and firmware updates from the wireless manufacturer should be applied to the WAP and affected wireless cards as soon as possible after release to keep the security updated.

Resources:

- CIO-072, Commonwealth's Enterprise UserID and Password Policy:
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13212/>

END